REMARKS/ARGUMENTS

The present application discloses a document repository system in which the originator of the document is able to ensure the integrity and security of its document filed with a third party repository without having to trust the administrator of that repository. In this repository system, the document originator and the repository administrator have vault environments which are secure extensions of their respective work spaces. The vault of the document originator encrypts a document that it receives from the originator, prior to forwarding it on to the vault of the repository to maintain the document secure from the repository administrator. When a request is made to view the document, it is made from the vault which is a secure extension of the requesting party's work space to the repository's vault. The repository's vault retrieves a copy of the encrypted document which is forwards, along with the requester's identity, to the originator's vault. The originator's vault verifies that the requester is authorized to view the document from the access control list using an access control list identifying access ownership privileges for the document stored in the vault itself. The originator's vault decrypts the document and forwards the decrypted document directly to the requester's vault. Therefore the repository administrator never handles the decrypted documents or the encrypting and decrypting of the documents.

The repository system also maintains the information on authorized user access secure from any actions of the third party administrator of the repository. To this end, the system includes a communications environment that houses a first agent program in the data repository system which is a secure extension of the work space of the depositor's computer and a second agent program which is a secure

extension of the work space of a first user computer with access privileges to the electronic data file. A manifest is accessible to and maintained by the first agent program. The first user computer has a record of its access privileges to the electronic data file which is accessible to and maintained by the second agent program. When changes are made to the manifest affecting the first user computer's access privileges to the electronic data file, these changes are communicated from the first agent program to the second agent program so that the first user computer's record of its access privileges can be updated. The first agent program is also able to verify the first user computer's access privileges to the electronic data file before the electronic data file is released to the second agent program.

Claim Rejections Under 35 USC 102

The original claims in the application were all rejected under 35 USC 102(b) as being anticipated by the Frisch reference entitled "Essential system Administration" 2nd Edition published by O'Reilly & Associates, Inc.

The applicant's attorney did not find material in the sections cited by the Examiner that deals with preventing access by the repository administrator to a directory of authorized users of data stored in the repository. In fact it would appear from at least one of the sections that a repository administrator would have access to such a repository directory. In rejecting claim 2, the Examiner cites material beginning on page 246 of the Frisch reference. This material makes it clear that the repository administrator has access to the directory when running a program called "crack". Therefore the repository administrator in a third party repository would

have access to the directory. (Also, see page 226 of the Frisch reference about the system administrator's ability to grant access to the "root" account.)

For the above reasons all claims in the application are allowable over the Frisch reference. Independent claim 1 now incorporates the subject matter of cancelled dependent claim 2 which calls for a first agent program which is a secure extension of the depositors computer and a second agent program which is a secure extension of the first user computer. Independent claims 10, 11, 12 and 14 all call for a data repository in which data is secure from the repository administrator.

Objections to the Drawings

The attached copy of Figure 3 of the drawings, with proposed changes marked in red, is submitted for the Examiner's approval.

Objections to the Specification

The changes by the Examiner to pages 5 and 6 have been adopted. The referral to "Figure 4" on page 12, has been changed to -- Figures 4A and 4B -- which are contained in the drawing. Also, the grammar of the sentence beginning on line 20 has been corrected.

The selection of the appropriate encryption algorithm to protect the documents is well within the ability of those skilled in the art.

For the above reasons, it is respectfully submitted that the claims are allowable over the prior art and the application is in condition for allowance. Therefore, it is requested that the application be reconsidered, allowed and passed to issue.

Respectfully submitted,

James E. Murray - Attorney
Reg. No.: 20,915
Telephone No.: (845) 462-4763

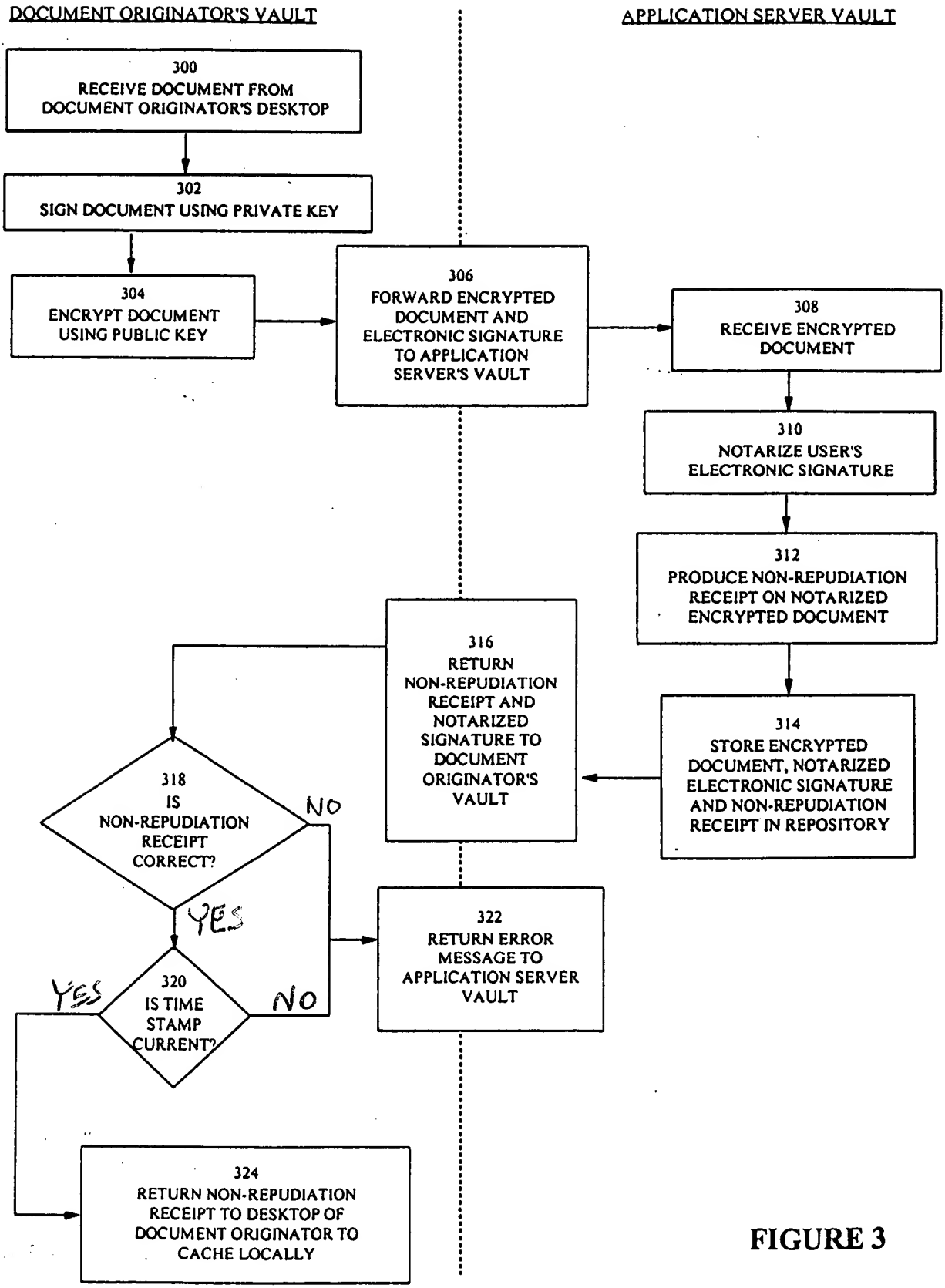

FIGURE 3

SN 09/459,240 filed 12/10/99